* Background Did the presentation adequately explain
  + What is the 2FA/MFA?

2FA is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of factors to an [authentication](https://en.wikipedia.org/wiki/Authentication) mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

* + Who uses it

finance, healthcare, law enforcement, and government

* + How does it work?
    - Different forms of two-factor authentication
      * Physical Authentication Keys(U2F)
        + A common two-factor combination is a password + some personal item, such as a USB shield for online banking. The user plugs the USB shield into the laptop and enters the password to log in to online banking.
        + It is a minor USB key that you put on your keychain. Whenever you want to log into your account from a new computer, you have to insert the USB key and press the button on it. That is it - no code needed. In the future, these devices should work with NFC and Bluetooth to communicate with mobile devices that do not have USB ports.
        + pro:

This solution works better than SMS verification and one-time-use codes because it cannot be intercepted and messed

Con:

The user cannot carry the USB shield at all times, and it is easy to lose it. In contrast, mobile phones are an excellent alternative.

* + - * SMS
        + Many services require users to receive SMS messages when they login to their accounts. The SMS message will contain a one-time code, and the user needs to enter this code as a second authentication method to log in to the account.

Pro:

Compared with U2F, it is more portable. Because users do not need to carry extra equipment, most people have cell phones. Some services even dial a phone number and have an automated system to speak the code, and landline numbers that cannot receive text messages can also receive codes.

Cons:

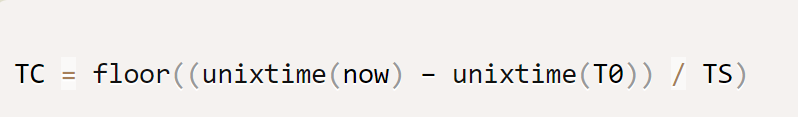
There is a big problem with SMS. Attackers can use SIM swapping attacks to access the security codes or intercept them.

* + - * Authenticator Apps(TOTP)

The full name of TOTP is Time-based One-time Password. It is recognized as a reliable solution and has been written into the international standard RFC6238.

Authentication apps work by using a mobile app to generate an authentication code. Unlike SMS, the application does not require the user to access the wireless network. Any internet connection is sufficient to access the account. How it works is that when the user turns on two-factor authentication, the server will generate a secret key. The server prompts the user to scan the QR code (or use other methods) to save the key to the user's mobile phone. That is to say, the server and the user's mobile phone now have the same key. Note that the key must be bound to the phone. Once the user changes the phone, a brand new key must be generated. When the user is ready to log in, the mobile client uses this key and the current timestamp to generate a hash with a default validity period of 30 seconds. The user submits this hash to the server within the validity period. Finally, the server also uses the key and the current timestamp to generate a hash compared with the hash submitted by the user. As long as the two are inconsistent, the login is denied.

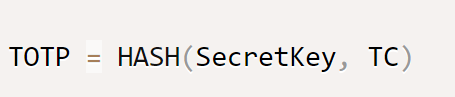
* + - * + Google Authenticator
    - How 2FA stops the attack
      * Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.
      * Two-factor authentication adds an extra layer of security to the authentication process by making it harder for attackers to gain access to personal devices or online accounts since passwords alone are not enough even if a victim's password is hacked View through authentication. Two-factor authentication has long been used to control sensitive systems and data access. Online service providers increasingly use 2FA to protect their users' credentials from hackers who steal password databases or use phishing campaigns to obtain users' passwords.
      * Hackers often send emails containing links to malicious websites designed to infect users' computers or convince them to enter their passwords. Once obtained, the password can be used by anyone managing hacking attempts. 2FA fights phishing by adding a second layer of verification after entering a password.
      * Also, hackers often manipulate users into giving up their passwords. By impersonating an IT professional at the user's company, they can trust the user before asking for login credentials. 2FA prevents this by verifying the location and IP of each login attempt after entering the password.
* Technical merit. Did the topic contain an adequate degree of technical content (e.g., code, data, equations, graphs, charts, etc). Were key concepts explained?
  + TOTP's algorithm
    - How to ensure that both the mobile client and the server get the same hash during the 30 seconds:



In the above formula, TC represents a time counter, unixtime(now) is the current Unix timestamp, and unixtime(T0) is the timestamp of the agreed start time. The default is 0, which is January 1, 1970. TS is the length of time the hash is valid for; the default is 30 seconds. Therefore, the above formula becomes the following form.

Therefore, as long as it is within 30 seconds, the value of TC is the same. The premise is that the time of the server and the mobile phone must be synchronized.

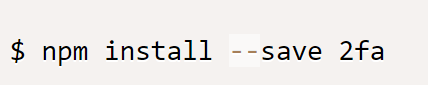
Next, the hash can be calculated.



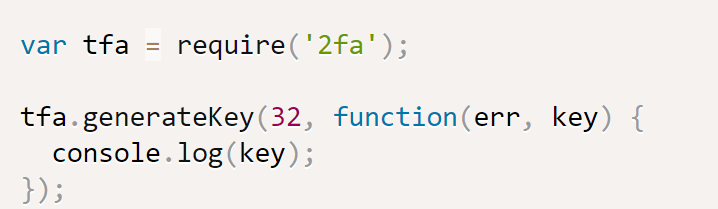
HASH is the agreed hash function, and the default is SHA-1.

Implementation of TOTP

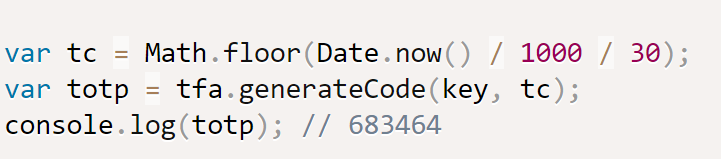
Implement 2fa in JavaScript to demonstrate the code. First, install this module.



Then, generate a 32-character key.



The hash can now be generated.



* + Types of 2FA hacking:
    - Supply Chain Attacks: Vendor attacks that target the supply chain of a software or software that is a service to the vendor. The goal is to access source codes. The most famous attack in recent years is the [SolarWinds](https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html) attack, various code components of the company were infected, and employees of the company downloaded the virus software by accident. Hackers modify authentication credentials and use tools to modify environment variables, allowing hackers to track and modify target IP addresses to obtain sensitive information.
    - Compromised MFA authentication:
    - Man-in-the-middle attacks (MITM):
  + Evilginx2:
    - is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

give examples of attacks and how 2FA stops them. Also give some guidelines of good and bad 2FA, and examples of sites that use 2FA

Summary:

The advantage of two-factor authentication is that it is much more secure than a simple password login. Even if the password is leaked, the account is safe as long as the phone is still there. Various password cracking methods are invalid for two-factor authentication.

The disadvantage is that it takes one more step to log in, which is time-consuming and troublesome, and the user will feel impatient. Moreover, it does not mean that the account is safe; an intruder can still hijack the entire session by stealing the cookie or token.

One of the biggest problems with two-factor authentication is account recovery. Once a user forgets his password or loses his phone, he must bypass two-factor authentication to restore login, which creates a security hole. Unless preparing two sets of two-factor authentication, one is used for logging in, and the other is to restore the account.

<https://www.merchantfraudjournal.com/two-factor-authentication-work/>

<https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa>

<https://www.howtogeek.com/232598/5-different-two-step-authentication-methods-to-secure-your-online-accounts/>

<https://www.secsign.com/usb-authentication-keys-tokens-bad-idea/>

<https://www.usenix.org/system/files/soups2019-reese.pdf>